CLAIMS

1. Method for performing the analysis and/or selective modification and/or selective filtering of data packets (PD) passing through a device (D) placed on an edge in a computer network (R), said device (D) comprising a processor (P) that runs a compiler (C) and a piece of software (L) in accordance with a security policy (PS), said software (L) being designed to filter said data packets (PD), authorizing or not authorizing their passage in accordance with said security policy (PS), said method being characterized in that it comprises the following steps:

- the step of defining said security policy (PS) by means of portable agents (A1) written in a computer language (Li) that is independent of the language of said processor (P) and dedicated to the analysis and/or the selective modification and/or the selective filtering of said data packets (PD);

- the step, for said software (L), of automatically calling said compiler (C) in order to perform a compilation for translating said portable agents (A1) into executable agents (A2) written in the language of said processor (P);

- the step of running said software (L) in order to filter said data packets (PD) passing through said device (D), authorizing or not authorizing their passage in accordance with said security policy (PS);

- the step of analyzing said data packets (PD) authorized by said software (L) to pass through said device (D), by executing said agents executable by said processor (P); and/or

- the step of selectively modifying said data packets (PD) authorized by said software (L) to pass through said device (D), by executing said agents executable by said processor (P); and/or

- the step of selectively filtering said data packets (PD) authorized by said software (L) to pass through said device (D), by executing said agents (A2) executable by said processor (P).

2. Method according to claim 1, characterized in that said security policy (PS) also includes a definition of the various objects of said computer network (R).

3. Method according to either of claims 1 and 2, characterized in that said security policy (PS) also includes a definition of the various services of said computer network (R).

4. Method according to any of claims 1 through 3, characterized in that said security policy (PS) also comprises a definition of the various users (U_i) of said computer network (R).

5. Method according to claim 4, characterized in that it also includes the step of generating configuration parameters, making it possible to configure said portable agents (A1) based on said users (U_i) of said computer network (R).

6. Method according to any of claims 1 through 5, characterized in that said security policy (PS) also includes a definition of said device (D).

7. Method according to any of claims 1 through 6, characterized in that said computer language (Li) is a low-level language that is dedicated to operations on said data packets (PD) of said computer network (R) and that makes it possible to monitor and to limit the possible actions of said portable agents (A1) inside said device (D).

8. Method according to any of claims 1 through 7, characterized in that it also includes the step of defining, in a server remote from said device (D), said security policy (PS).

9. Method according to any of claims 1 through 7, characterized in that it also includes the step of defining, in said device (D), said security policy (PS).

10. Method according to any of claims 1 through 9, characterized in that it also includes the step of authenticating the non-authenticated user or users (U_i) of said device (D).

11. Method according to claim 10, characterized in that said security policy (PS) also includes a definition of said authenticated users (U_i) of said device (D).

12. Method according to claim 11, characterized in that it also includes the step of authenticating said non-authenticated user or users (U_i) of said device (D) using an identification means associated with said device (D).

13. Method according to claim 11, characterized in that it also includes the step of authenticating said non-authenticated user or users (U_i) of said device (D) using a client/server application whose server application is contained in said device (D).

14. Method according to any of claims 1 through 13, characterized in that it also includes the step of executing functions (F) from a function library (BF) contained in said software (L) and called by said executable agents (A2).

15. Method according to claim 14, characterized in that it also includes the step of executing specialized functions (F), from said function library (BF), for managing a cache of said data packets (PD).

16. Method according to claim 15, characterized in that the management of said cache of said data packets (PD) comprises the following steps:

- the step of storing in said cache, after the execution of said executable agents (A2), packet information concerning said data packets (PD), as well as said data packets (PD) themselves when they have been modified during said execution;

- the step, upon the arrival of an incoming packet in said device (D), of verifying, based on said packet information stored in said cache, whether said incoming packet is a packet that has already been received;

- the step, when said incoming packet is not a packet that has already been received, of executing said executable agents (A2);

- the step, when said incoming packet is a packet that has already been received, of determining, using said packet information stored in said cache, whether said already received packet has been modified by said executable agents (A2);

- the step, when said already received packet has been modified by said executable agents (A2), of transmitting a version of said already received packet stored in said cache to said computer network (R), without executing said executable agents (A2);

- the step, when said previously received packet has not been modified by said executable agents (A2), of transmitting said incoming packet as is to said computer network (R), without executing said executable agents (A2).

17. Method according to any of claims 14 through 16, characterized in that it also includes the step of executing specialized functions (F), from said function library (BF), for managing the network and transport layers of the communication protocol used.

18. Method according to claim 17 characterized in that the management of said network and transport layers comprises the following steps:

- the step of storing protocol information from said network and transport layers of said data packets (PD) passing through said device (D), for the purpose of monitoring the various flows of said data packets (PD);

- the step of storing any modifications of said data packets (PD) performed by said executable agents (A2);

- the step of updating said protocol information from said network and transport layers of said data packets (PD) passing through said device (D), based on said protocol information and said stored modifications, in said data packets (PD) so as to maintain consistency in the flows of said data packets (PD).

19. Method according to any of claims 14 through 18 characterized in that it also includes the step of executing specialized functions (F), from said function library (BF), for searching for regular patterns and expressions.

20. Method according to any of claims 14 through 19 characterized in that it also includes the step of executing specialized functions (F), from said function library (BF), for communicating between said executable agents (A2).

21. Method according to any of claims 14 through 20 characterized in that it also includes the step of executing specialized functions (F), from said function library (BF), for communicating between said executable agents (A2) and said objects of said computer network (R).

22. Method according to any of claims 14 through 21 characterized in that it also includes the step of associating specialized hardware components (CM) of said device (D) with functions (F) from said function library (BF) in order to accelerate the execution of said functions (F).

23. Method according to any of claims 1 through 22 characterized in that it also includes the step of modifying said security policy (PS) by executing said agents executable by said processor (P).

24. System for performing the analysis and/or selective modification and/or selective filtering of data packets (PD), said system comprising:

a device (D) passed through by said data packets (PD) and placed on an edge in a computer network (R), said device (D) comprising a processor (P) that runs a compiler (C) and a piece of software (L) in accordance with a security policy (PS), said software (L) comprising filtering means for filtering said data packets (PD) passing through said device (D), authorizing or not authorizing their passage in accordance with said security policy (PS), and,

portable agents (A1) designed to define said security policy (PS), written in a computer language (Li) that is independent of the language of said processor (P) and dedicated to the analysis and/or selective modification and/or selective filtering of said data packets (PD);

said compiler (C) being automatically activated by said software (L) in order to translate said portable agents (A1) into executable agents (A2) written in the language of said processor (P), said executable agents (A2) being executed by said processor (P) in order to:

analyze said data packets (PD) authorized by said software (L) to pass through said device (D), and/or

selectively modify said data packets (PD) authorized by said software (L) to pass through said device (D), and/or

selectively filter said data packets (PD) authorized by said software (L) to pass through said device (D).

25. System according to claim 24, said system being such that said security policy (PS) also includes a definition of the various objects of said computer network (R).

26. System according to either of claims 24 and 25, said system being such that said security policy (PS) also includes a definition of the various services of said computer network (R).

27. System according to any of claims 24 through 26, said system being such that said security policy (PS) also includes a definition of the various users (U_i) of said computer network (R).

28. System according to claim 27 characterized in that it also includes means for generating configuration parameters for configuring said portable agents (A1) based on said users (U_i) of said computer network (R).

29. System according to any of claims 24 through 28, said system being such that said security policy (PS) also includes a definition of said device (D).

30. System according to any of claims 24 through 29, said system being such that said computer language (Li) is a low-level language that is dedicated to operations on said data packets (PD) of said computer network (R) and that makes it possible to monitor and to limit the possible actions of said portable agents (A1) in said device (D).

31. System according to any of claims 24 through 30 characterized in that it includes a server, remote from said device (D), for defining said security policy (PS).

32. System according to any of claims 24 through 30, said system being such that said device (D) includes administrative means for defining said security policy (PS).

33. System according to any of claims 24 through 32 characterized in that it includes means for authenticating the non-authenticated user or users (U_i) of said device (D).

34. System according to claim 33, said system being such that said security policy (PS) also includes a definition of said authenticated users (U_i) of said device (D).

35. System according to claim 34 characterized in that said device (D) includes an identification means for authenticating said non-authenticated user or users (U_i) of said device (D).

36. System according to claim 34 characterized in that said device (D) includes a server application of a client/server application designed to authenticate said non-authenticated user or users (U_i) of said device (D).

37. System according to any of claims 24 through 36 characterized in that said software includes a function library (BF) whose functions (F) are called by said executable agents (A2).

38. System according to claim 37, said system being such that said function library (BF) also includes specialized functions (F) for managing a cache of said data packets (PD).

39. System according to claim 38 characterized in that said cache of said data packets (PD) comprises:

a memory for storing, after the execution of said executable agents (A2), packet information concerning said data packets (PD), and for storing said data packets (PD) themselves;

verification means for verifying, based on said packet information stored in said cache, whether an incoming packet is a packet that has already been received and whether it has been modified by said executable agents (A2);

activation means for activating, based on the verifications performed by the verification means,

either transmission means for transmitting a data packet (PD) stored in said memory to said computer network (R) without modification

or transmission means for transmitting an incoming packet to said computer network (R) without modification.

40. System according to any of claims 37 through 39, said system being such that said function library (BF) also includes specialized functions (F) for managing the network and transport layers of the communication protocol used.

41. System according to claim 40, said system being such that said device (D) comprises:

at least one memory

for storing protocol information from said network and transport layers of said data packets (PD) passing through said device (D), for the purpose of monitoring the various flows of said data packets (PD),

and for storing any modifications of said data packets (PD) performed by said executable agents (A2),

and means for updating said protocol information from said network and transport layers of said data packets (PD) passing through said device (D), based on said protocol information and said stored modifications, in said data packets (PD) so as to maintain consistency in the flows of said data packets (PD).

42. System according to any of claims 37 through 41, said system being such that said function library (BF) also includes specialized functions (F) for searching for regular patterns and expressions.

43. System according to any of claims 37 through 42, said system being such that said function library (BF) also includes specialized functions (F) for communicating between said executable agents (A2).

44. System according to any of claims 37 through 43, said system being such that said function library (BF) includes specialized functions (F) for communicating between said executable agents (A2) and said objects of said computer network (R).

45. System according to any of claims 37 through 44, characterized in that said device (D) includes specialized hardware components (CM) associated with functions (F) from said function library (BF), in order to accelerate the execution of said functions (F).

46. System according to any of claims 24 through 45, said system being such that said executable agents (A2) executed by said processor (P) modify said security policy (PS).